from dividing the relied-upon "traitor subset" at col. 4, lines 13-16 ("two new subsets are ***arbitrarily*** formed", emphasis mine).

Next consider that apart from never dividing the relied-upon traitor subset in the first place, Schwenk nowhere considers determining whether it might contain not one but two traitors, much less as a precondition for dividing the traitor subset. Indeed, Schwenk, col. 4, lines 35-39 suggests that to find more traitors, more leaves of its tree must be used, i.e., the method of Schwenk multiplies its scheme, instead of dividing a traitor subset, to find two or more traitors.

Accordingly, as the above careful analysis of what Schwenk actually teaches shows, Claim 1 and, hence, its respective dependent claims are patentable over Schwenk.

With particular respect to the allegation that Schwenk, col. 3, lines 36-58 teach everything in Claim 8 except encrypting a false key, this likewise appears to be incorrect, starting with the fact that Claim 8 explicitly states that its elements are a non-limiting way to generate the set of subsets, a limitation not mentioned in the Office Action. The relied-upon tree of Schwenk has leaves, each of which represents a receiver, and nodes, each of which is a group key that is encrypted using the private keys of the receivers. Nowhere does Schwenk mention how this tree gets generated. It appears that receivers (with their private keys) are arbitrarily assigned group keys, although the relied-upon portion of Schwenk doesn't say. What matters is that Schwenk plainly does not disclose anything remotely close to Claim 8 for purposes of generating subsets.

Apart from the fact that the relied-upon portion of Schwenk is not used for generating subsets, it does not teach what has been alleged. Specifically, the relied-upon portion of Schwenk nowhere mentions a revoked set, much less using it as claimed, and significantly (and not surprisingly) the limitation of "revoked

set" has been elided over in the rejection. Furthermore, Claim 8 does not merely encrypt a false key as allegedly taught in the secondary reference, but it also encrypts a session key and it does so using something specifically claimed but not mentioned in the rejection, namely, a set of subset keys.

Consider next Claim 9, which does not merely recite "assigning keys from nodes above the receiver" as alleged in the rejection but rather requires each receiver to be assigned keys from all nodes in a direct path between a leaf representing the receiver and the root of the tree. This particular limitation has not been mentioned in the rejection.

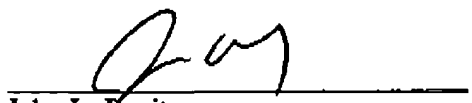
The limitation of Claim 10 has not been specifically addressed to date in this prosecution. Suffice it to say that nothing in Schwenk appears to suggest, much less teach, that each node is associated with a set of labels, and that each receiver is assigned labels from all nodes hanging from a direct path between the receiver and the root but not from nodes in the direct path.

Likewise, the allegation that Schwenk, col. 4, teaches initializing a spanning tree fails to account for several salient limitations of Claim 11, such as that the spanning tree is defined by a revoked set, is initialized by a cover tree, with nodes from the cover tree being iteratively removed and with nodes being added to the cover tree until the cover tree T has at most one node. Probably these limitations have not been mentioned in the rejection because in fact they do not appear in Schwenk.

The arguments above apply to the rejections of Claims 18, 19, and 28. Applicant's previous arguments regarding the lack of a suggestion to combine references are incorporated herein.

The Examiner is cordially invited to telephone the undersigned at (619) 338-8075 for any reason which would advance the instant application to allowance.

Respectfully submitted,



John L. Rogitz
Registration No. 33,549
Attorney of Record
750 B Street, Suite 3120
San Diego, CA 92101
Telephone: (619) 338-8075

JLR:jg

1053-122.AM2